European Journal of Physics

REVIEW • **OPEN ACCESS**

Towards a quantum internet

To cite this article: Wolfgang Dür *et al* 2017 *Eur. J. Phys.* **38** 043001

OPEN ACCESS
IOP Publishing

Made open access 7 November 2017
European Journal of Physics

Eur. J. Phys. **38** (2017) 043001 (17pp) https://doi.org/10.1088/1361-6404/aa6df7

Review

Towards a quantum internet

Wolfgang Dür[1,3], Raphael Lamprecht[1] and Stefan Heusler[2]

[1] Institut für Theoretische Physik und Institut für Fachdidaktik, Bereich DINGIM, Universität Innsbruck, Technikerstrasse 21a, A-6020 Innsbruck, Austria
[2] Institut für Didaktik der Physik, Universität Münster, Germany

E-mail: wolfgang.duer@uibk.ac.at

Received 19 January 2017, revised 11 April 2017
Accepted for publication 19 April 2017
Published 12 May 2017

CrossMark

Abstract
A long-range quantum communication network is among the most promising applications of emerging quantum technologies. We discuss the potential of such a quantum internet for the secure transmission of classical and quantum information, as well as theoretical and experimental approaches and recent advances to realize them. We illustrate the involved concepts such as error correction, teleportation or quantum repeaters and consider an approach to this topic based on catchy visualizations as a context-based, modern treatment of quantum theory at high school.

Keywords: quantum information, quantum communication, visualizations of quantum theory

(Some figures may appear in colour only in the online journal)

1. Introduction

It is hard to imagine our modern world without the internet, which is a central communication and information network we use on a daily basis for work, research and in our leisure time. The world-wide-web, as central component of the modern internet, was initially planned only as a tool to communicate research results with CERN, but has become a central pillar of our modern society. This constitutes one of the most important examples where fundamental research leads to unforeseen and unexpected applications.

The basic functionality of the internet is the transmission of classical information between two (or more) communication partners. However, as Landauer pointed out, information is physical, i.e. needs to be encoded or stored using some physical system, like for example ordering of magnetic domains. Physical systems such a light or atoms, in turn, need at a microsopic level be described by quantum theory. While this is known for almost a

[3] Author to whom any correspondence should be addressed.

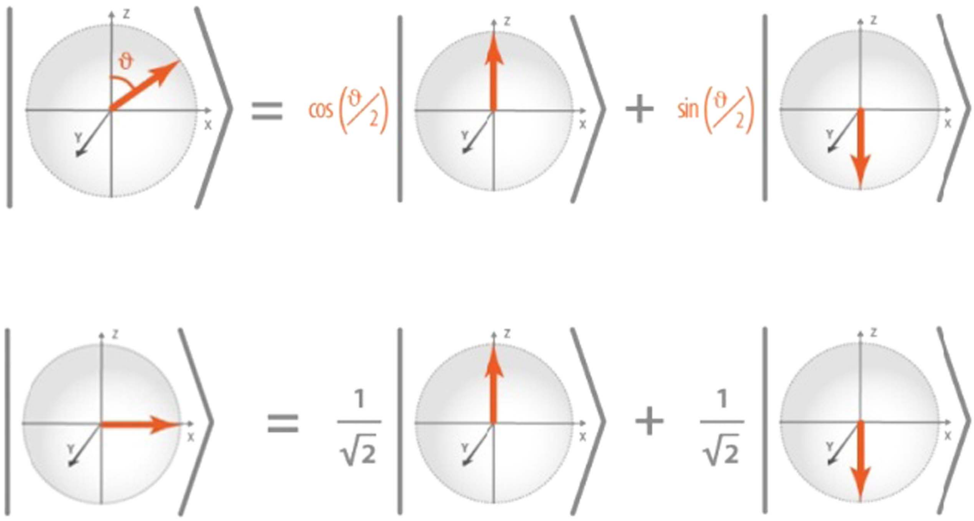

Figure 1. Bloch sphere representation of different superposition states. Quantum states are represented by vectors of unit length, where states $|0\rangle$ and $|1\rangle$ correspond to vectors pointing in $\pm z$ direction respectively. An equal superposition state $(|0\rangle + |1\rangle)/\sqrt{2}$ corresponds to an arrow pointing in x-direction, while different values of the coefficients correspond to vectors pointing in different directions. Taking complex values into account would require a sphere rather than a circle, which is however not required for high-school purposes.

century, it was only realized about two decades ago that the strange and counter-intuitive features of quantum physics can be harnessed in practice. It was discovered that not only classical information but also quantum information exists. The bit as a basic information carrier needs to be replaced by the qubit, which shows new and fundamentally different features. With increasing miniaturization, the situation where quantum effects cannot be neglected will emerge. In contrast to classical bits, quantum states can be in a superposition of two (or more) possibilities, and act in a probabilistic manner when measured. These features open the way to new methods and protocols to transmit and manipulate (quantum) information, including quantum communication [1] and quantum computation [2], with teleportation [3] and quantum cryptography [4] constituting well-known examples.

While initially the counter-intuitive features of quantum mechanics gave rise to thought experiments such as Schrödinger's cat [5], recent experimental progress now allows us to manipulate single atoms and photons [6, 7] and to observe and even use their strange features in practice. Quantum technologies are believed to play a key role in future. This can e.g. be seen by the planned one billion Euro flagship program in Europe to further develop these technologies and applications. While a full-scale quantum computer is still technologically very challenging, a quantum communication network (a 'quantum internet') has become a realistic possibility and is one of the most promising applications of an emerging quantum technology [8]. On the one hand, it allows for secure classical communication via quantum key distribution—a task of fundamental importance in our communication-based society. On the other hand, the transmission of *quantum information* is also possible, which might find applications in distributed quantum computation or distributed sensing networks.

In this article we provide an overview over different ways to realize such a long-distance quantum communication network. We discuss possible applications, theoretical and

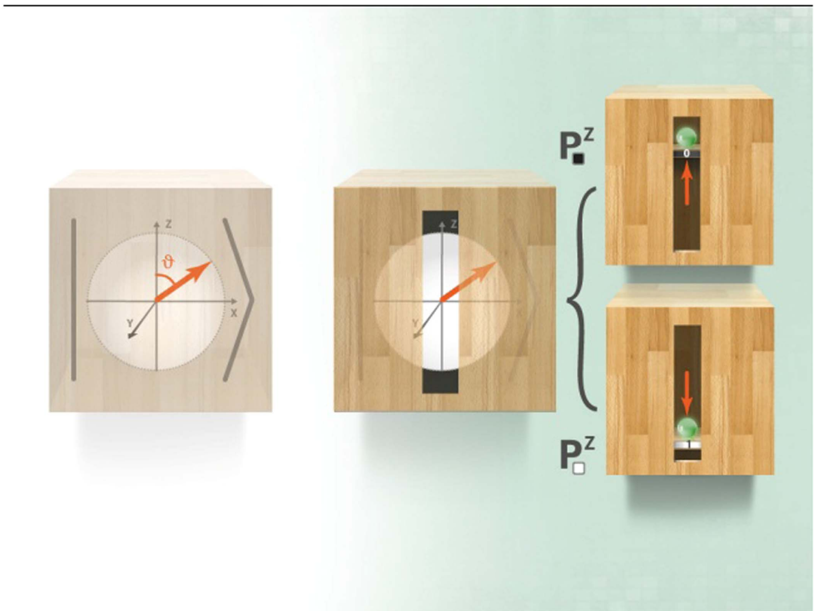

Figure 2. Illustration of a z-measurement (observable σ_z) performed on a qubit in state $|\psi\rangle = \cos\frac{\vartheta}{2}|0\rangle + \sin\frac{\vartheta}{2}|1\rangle$. The state vector is not oriented in slit direction, and hence the measurement process enforces a rotation of the vector in positive or negative z-direction. This leads to a random measurement result $|0\rangle$ or $|1\rangle$, with probability $p_0 = \cos^2\frac{\vartheta}{2}$ and $p_1 = \sin^2\frac{\vartheta}{2}$, and a change of the state vector after the measurement.

experimental challenges and recent advances. At the same time, we also consider the possible treatment of such a topic in high school. We illustrate the underlying concepts with catchy visualizations, and discuss the possibility to use the treatment of the quantum internet as a context-based approach to modern quantum theory.

2. Potential applications of a quantum internet

Before we can consider different applications of a quantum communication network, we need to discuss the basic features of qubits and their main differences to classical bits [9–13].

2.1. Properties of qubits

The qubit is the generalization of the classical bit. It provides an abstract description of a physical object with one characteristic property, that can assume the possible values $|0\rangle$ or $|1\rangle$, such as spin up or spin down of an electron. In contrast to a classical bit, a qubit can also be in a superposition of the two basis states, $\alpha|0\rangle + \beta|1\rangle$ which can be illustrated using the Bloch sphere or Bloch circle (see figure 1). In a sense, the quantum system is in two possible states simultaneously. For the spin, this just signifies that the spin can be directed in any direction in space. A measurement in the basis $\{|0\rangle, |1\rangle\}$ destroys the superposition, and leads either to the result $|0\rangle$ or $|1\rangle$, although in general the outcome of each measurement is random and cannot be predicted. Only the statistical behavior for many repetitions (i.e. the probabilities p_0, p_1) are determined by quantum theory as $p_0 = |\alpha^2|$ for the result $|0\rangle$ and $p_1 = |\beta^2|$ for the

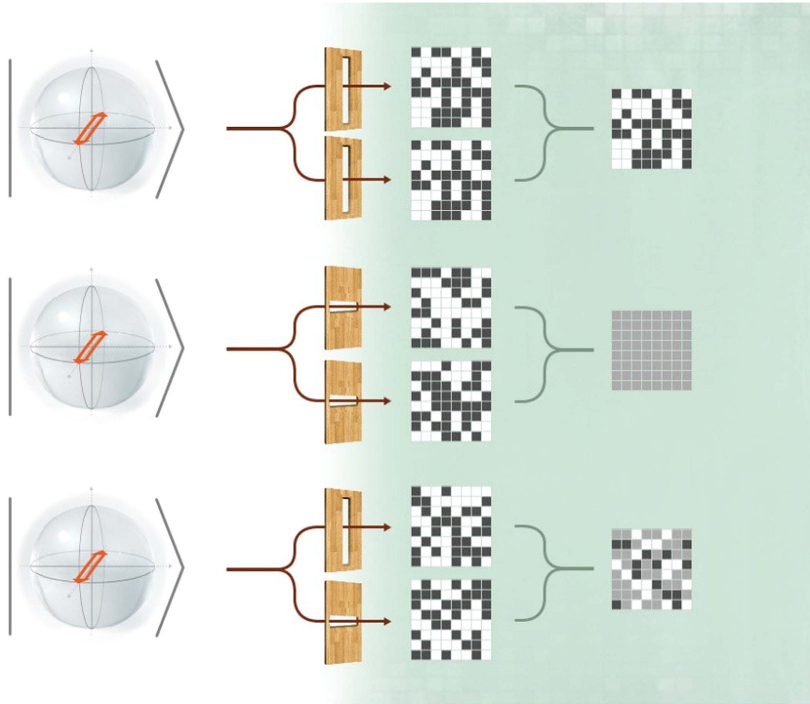

Figure 3. Correlations in an entangled state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$. Independent of the position of the two qubits, one finds a perfect correlation between the two random measurement outcomes when performing a measurement in the z-basis. A measurement in the y-basis yields perfect anticorrelation, which can be seen by rewriting the quantum state as $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0_y\rangle|1_y\rangle + |1_y\rangle|0_y\rangle))$, where $|0_y\rangle = (|0\rangle + \mathrm{i}|1\rangle)/\sqrt{2}$, $|1_y\rangle = (|0\rangle - \mathrm{i}|1\rangle)/\sqrt{2}$. When the measurement basis at the two qubits do not coincide, there are no or only weak correlations.

result $|1\rangle$. Thus, a measurement leads to a change of the quantum state that depends on the measurement outcome (see figure 2 for an illustration). These properties of the qubit constitute the main differences between quantum theory and classical theories [9, 10, 12], and are the basis of many applications of quantum information theory.

A qubit can be realized not only by the spin, but in fact *all* physical systems which can be described by two basis states, including e.g. the polarization degree of freedom of a single photon, two electronic states of an ion (with all other degrees of freedom being frozen), or the position of an atom in a double well [9, 11, 12].

For systems of two and more qubits, the superposition principle leads to a new phenomenon that has no classical counterpart: entanglement. Entangled states such as

$$|\phi^+\rangle = (|0\rangle|0\rangle + |1\rangle|1\rangle)/\sqrt{2}, \tag{1}$$

have the curious feature that measurements on the individual constituents yield random outcomes, however the system as a whole shows a correlated behavior (see figure 3). Measurement outcomes of a z-measurement are random, but always coincide, independent of the distance between the two qubits. This non-local behavior is perhaps one of the most puzzling features of quantum mechanics, and has far-reaching consequences for our picture of

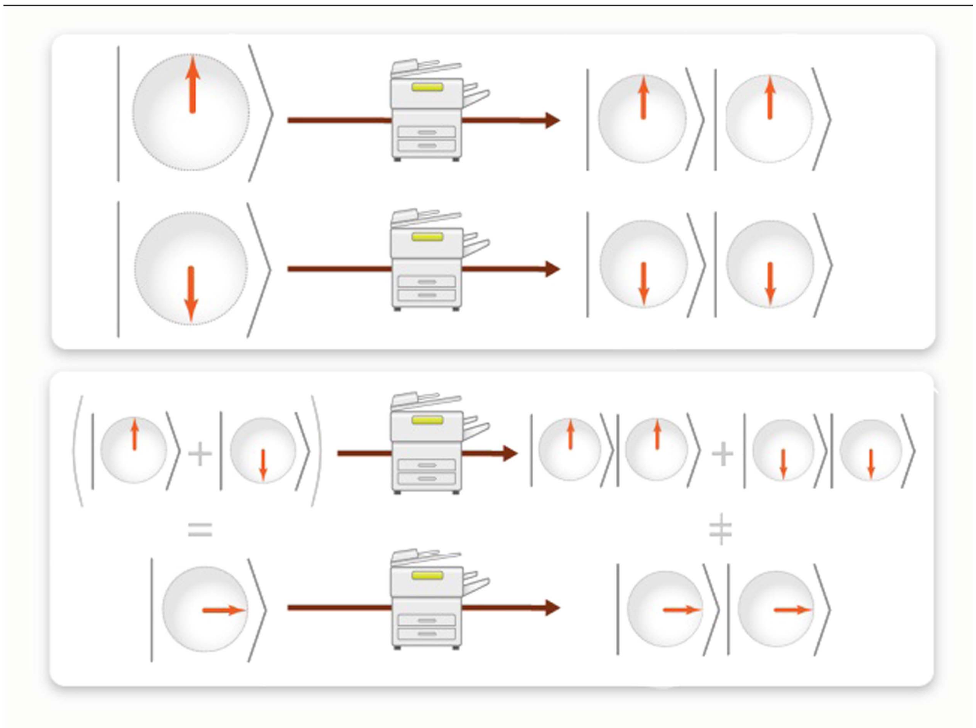

Figure 4. Illustration of the no-cloning theorem. Any copy machine capable of successfully cloning states $|0\rangle$ and $|1\rangle$ would provide an incorrect result for the superposition state $|0\rangle + |1\rangle$. Hence no perfect quantum cloning machine can exist.

nature. Note that also possible alternative theories beyond quantum mechanics need to include such a non-local behavior, since local (hidden variable) descriptions of the encountered correlations are in contradiction to experimental results [14].

Entanglement is not only puzzling from a philosophic point of view, but can in practice be applied as a key resource for different applications in the fast developing field of quantum information technology. Entangled states coexist as superposition at different positions of the network. If this is the case, the network does not just transmit classical information, but uses the key features of quantum mechanics to transmit quantum information, which leads to a higher degree of correlation between different positions of the network than any classical network can ever provide. Standard applications that can be realized using current technology are the generation of secret keys, and the transmission of (unknown) quantum information via teleportation. In the next section, these applications will be discussed more in detail.

2.2. Applications

The perhaps most important application of quantum communication is quantum cryptography [4]. The main purpose is to ensure secret communication of classical information, a problem that is not only important for governments or intelligence services, but also in everydays life when bank account or credit card details are transmitted. It is bad enough if the NSA or the secret service follow our communication, but if criminal gangs are involved this can end up in loss of money. Currently used classical cryptosystems such as RSA are based on the unproven assumption that certain mathematical operations (factorization of large integer numbers in its primes) are hard to perform on a classical computer. However, exactly this problem could be efficiently solved with a quantum computer, perhaps explaining the interest of researchers and governments.

Using quantum systems enables one not only to spoil the current technology of secret data transmission, but also to obtain a provable secure secret key, which can be used for secure communication. The reason for this can already be read off from the properties of a single qubit: any attempt to learn information yields to a change of the original quantum state that can eventually be detected. In other words, quantum information cannot be cloned—see figure 4 for an illustration. It is no problem to copy classical information (which is a challenge for protection of copyright) or basis states, however the copy machine will then produce incorrect results for a superposition state. This also implies that copyright for quantum states will never be a problem.

Other applications include the compression of classical information using pre-established entanglement. This so-called superdense coding allows to double the transmission rate. Secret voting or secret sharing are other examples, where entanglement is used to make information accessible if certain parties cooperate. Cloud computation might also be generalized to quantum systems.

How can we imagine a quantum internet in practice? At present, it seems unlikely that desktop quantum computers will be built in near future. However, quantum computation centers that can accept quantum inputs and deliver quantum outputs after the desired processing of the quantum information are imaginable. Moreover, distributed quantum computation, where small computational nodes are connected via quantum channels are discussed. Entanglement can also be used to quadratically improve the sensitivity of measurements, thereby allowing for the design of high-precession sensors with possible applications in research and real life. Atomic clock networks to improve positioning or navigation have already been proposed [15], and also other distributed sensing networks, e.g. for gravitational wave detection, are conceivable.

3. Quantum communication

The transmission of classical information is mostly realized using electromagnetical waves that are send over free space or optical fibers. Information is modulated or encoded in some way (e.g. in frequency, time or amplitude), and losses and noise are dealt with by re-amplifying the signal at regularly spaced repeater stations. Such an amplification, however is not possible for quantum information. The same principles, e.g. the no-cloning principle, that ensure security for key generation provide a fundamental problem for long-distance quantum communication, since amplification of the signal is not possible using classical means.

Quantum information can be *stored* using different systems, including light, ions, atoms, atomic ensembles, quantum dots, superconducting devices, NV centers etc. The method of choice to *transmit* quantum information, however, is based on sending photons over free space or optical fibers. Due to losses and dephasing errors, the communication distance is limited to distances of about a few hundred kilometers, which is not too bad, but by no means enough for a world wide quantum network. Different methods have been developed that allow in principle to overcome the limitations of non-amplification and to achieve long-distance communication: they are either based on quantum error correction, where quantum information is encoded in multiple systems and send through quantum channels, or on the

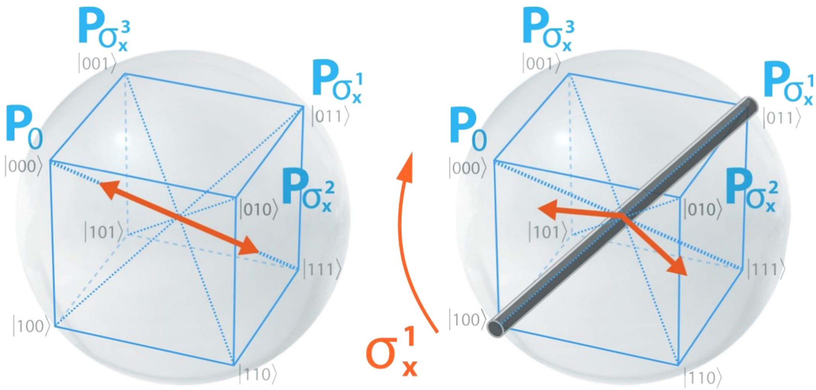

Figure 5. The entangled initial state $|\psi_L\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$ is visualized in a generalized eight-state Bloch sphere (left). Noise is introduced due to uncontrolled interactions with the environment (right). A projection onto one of the four subspaces $\{|0_L\rangle = |000\rangle, |1_L\rangle = |111\rangle\}$, $\{|100\rangle, |011\rangle\}$, $\{|010\rangle, |101\rangle\}$, $\{|001\rangle, |110\rangle\}$ followed by a bit-flip operation on none or one of the qubits (depending on the measurement outcome), allows to restore the initial state. In this visualization, the two-state Bloch sphere of figure 1 is turned into a tube connecting two diagonal corners of the cube. Projections onto two-dimensional subspaces correspond to the diagonals of the cube, and bit-flip operations change between diagonals.

generation of (known) long-distance entangled states that can be used to transmit quantum information via teleportation. We will discuss both methods in the following.

3.1. Quantum error correction and direct transmission

The basic idea of quantum error correction is to use several physical qubits to encode one logical qubit. For instance, consider the encoding of a single qubit into three physical ones, where codewords $|0_L\rangle = |000\rangle$ and $|1_L\rangle = |111\rangle$ are used and the logical qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is encoded as $|\psi_L\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$. A bit-flip error σ_x occurring on one of the systems, say the second, transforms the quantum state to an orthogonal one, $\sigma_x^{(2)}|\psi_L\rangle = \alpha|010\rangle + \beta|101\rangle$. In fact, one can deterministically distinguish between no error and an error occurring on system one, two or three, by projecting onto the two-dimensional subspaces, as all four possible states are pairwise orthogonal. Importantly, a quantum superposition within this subspace remains unknown and is not altered. Details for the error correction scheme and a visualization can be found in figure 5.

This code can be used to protect quantum information against single bit-flip errors. Also continuous errors can be treated, as the measurement process also leads to a digitization of errors. Similar schemes exists to protect quantum information against arbitrary errors. Each error can be seen as a superposition of elementary σ_x, σ_y, σ_z errors, where a code is constructed in such a way that each of the error operators transforms the logical qubit subspace to a different, orthogonal one. Five physical qubits suffice to protect a logical qubit against arbitrary single-qubit errors [2]. More complicated codes such as concatenated codes can be constructed to protect quantum information against multiple errors, where error rates of up to 25% can be dealt with.

To successfully transmit quantum information, one needs to perform error correction at regularly spaced intervals (repeater stations). Importantly, channel noise must not be too strong (about a few percent), otherwise error correction is no longer possible. In practice,

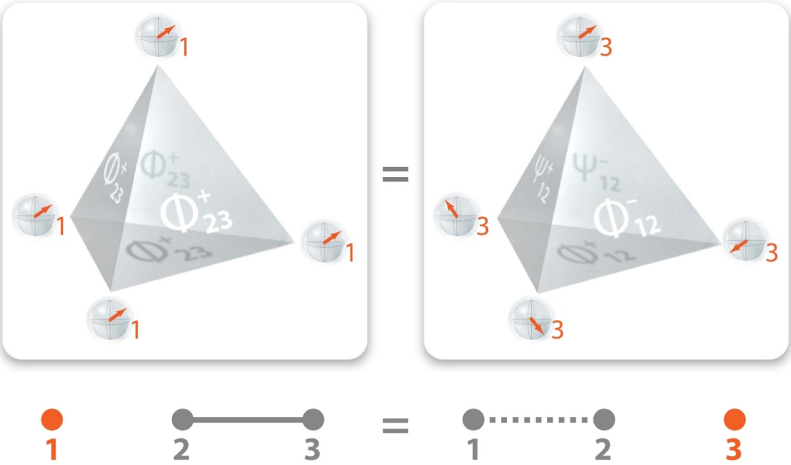

Figure 6. The product state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ of a qubit $\tilde{A}$ and a maximally entangled state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$ of qubits AB can equivalently be written as a superposition of one of the four Bell states for qubits $\tilde{A}A$, and a corresponding state for qubit B. We visualize each of the Bell states as one of the four faces of a tetrahedron, and the remaining third qubit as state that appears on the opposite vertex. In the left picture, where for qubits AB a Bell basis is used, there are identical single qubit states on all vertices. In the right picture, we decompose the state using the Bell basis for qubits $\tilde{A}A$, while different states for qubit B (which might be seen as 'coefficients') appear on the vertices in this decomposition. In the figure, qubits $\tilde{A}AB$ are labeled as 1, 2, 3.

however, also error detection and correction will suffer from errors in local operations, and one finds that acceptable error rates for local operations are of the order of 10^{-3}, and the required overhead in transmitted qubits is huge, making the application of such an approach challenging. Measurement-based implementations are currently discussed and promise much higher error tolerance [16].

3.2. Quantum teleportation

An alternative way to achieve transmission of quantum information is via teleportation [3], where an entangled state such as $|\phi^+\rangle$ (equation (1)) is used as a resource. While the name might be associated with science fiction, e.g. to beaming in Star Trek, teleportation is physically feasible and has in fact been experimentally demonstrated using different systems. In the following we will explain and illustrate how teleportation works [17].

Quantum entanglement or correlations in the form of a maximally entangled state $|\phi^+\rangle$ (equation (1)), shared between two parties Alice and Bob, are used to transmit the unknown state of an additional quantum system. In contrast to beaming, no matter, but only quantum information (or correlation) is transferred. Entanglement needs to be established beforehand, and an in-coupling measurement at Alice's side leaves the system at Bob's end in a state that is—up to a rotation—equivalent to the initial state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to be teleported from Alice to Bob. Once this is the case, the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ at Alice side is destroyed (Cloning is impossible!). However, two bits of classical information (the result of the in-coupling Bell measurement, i.e. a measurement in a basis of maximally entangled states) need to be transmitted. Otherwise, the state at Bob's side is completely random and contains no

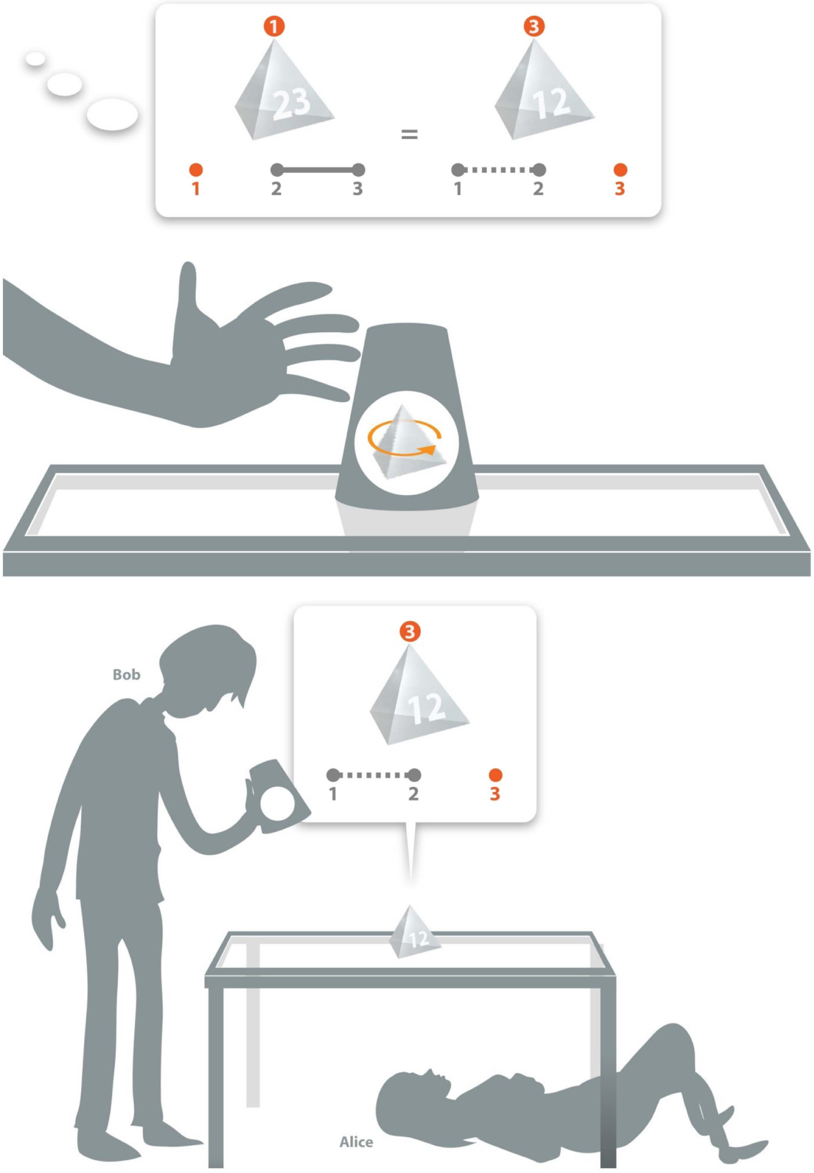

Figure 7. (a) (Upper part) Before the measurement takes place, the three-qubit state is in a superposition. The tetrahedron dice has not fallen yet. (b) (Lower part) The Bell measurement on qubits $\tilde{A}A$ at Alice side corresponds to fixing the state of qubits $\tilde{A}A$—the die is cast, and the dice lies on one of its faces. This in turn fixes the state of qubit B to the one of the opposite vertex of the tetrahedron. After transmitting the classical information about the result of the measurement outcome, Bob can rotate his qubit and restore the initial state of qubit $\tilde{A}$. In the figure, qubits $\tilde{A}AB$ are labeled as 1, 2, 3.

information. This makes sure that no information is transmitted faster than the speed of light, i.e. quantum mechanics respects this fundamental principle of relativity even though it is not explicitly included into its axioms.

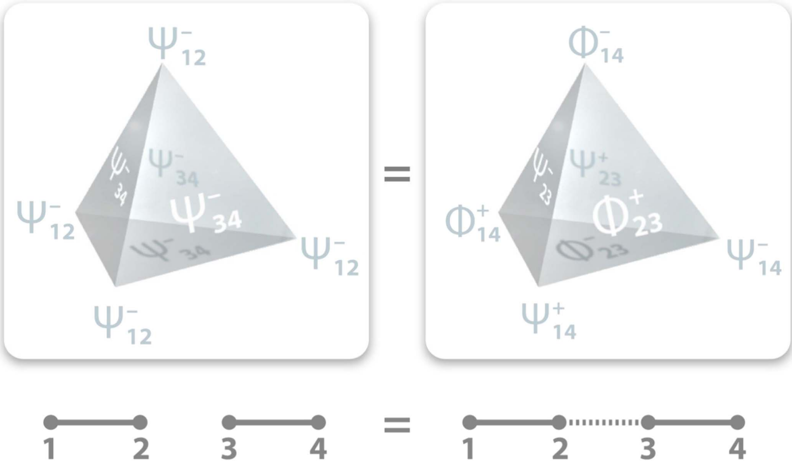

Figure 8. Similar as for a single qubit (see figures 6, 7), one can also teleport states that are themselves entangled to a third system C. We denote the Bell state of sytems $C\tilde{A}$ as (12), and the Bell state AB (the resource for teleporation) as (34). One may equally well consider the joint state as a superposition of Bell states of qubits (23) (the faces of the tetrahedron), with correpsonding Bell states (14) at opposite vertices (the 'coefficients' of this decomposition). Measuring qubit pair (23) fixes the dice, and hence also the resulting state for the qubit pair (14) which is—after the proper correction operation performed at 4 that depends on the outcome of the measurement—in a maximally entangled state. The entanglement is swapped, i.e. systems (14) (equivalently CB) are finally entangled.

To see how teleportation works more in detail, we start with the initial state $|\psi\rangle_{\tilde{A}}|\phi^+\rangle_{AB}$. Here, $|\psi\rangle_{\tilde{A}}$ is the initial state to be teleported from Alice to Bob, and $|\phi^+\rangle_{AB}$ is the entangled state provided by the quantum network to achieve this goal. With help of the Bell basis in system $\tilde{A}A$, defined by

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle),\ |\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \tag{2}$$

We can rewrite our initial state using $|00\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle + \phi^-\rangle)$, $|11\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle - \phi^-\rangle)$, $|01\rangle = \frac{1}{\sqrt{2}}(|\psi^+\rangle + \psi^-\rangle)$ und $|10\rangle = \frac{1}{\sqrt{2}}(|\psi^+\rangle - \psi^-\rangle)$. We find

$$\begin{aligned}|\psi\rangle_{\tilde{A}}|\phi^+\rangle_{AB} &= \alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\\ &= \frac{1}{2}[|\phi^+\rangle_{\tilde{A}A}(\alpha|0\rangle + \beta|1\rangle)_B + |\phi^-\rangle_{\tilde{A}A}(\alpha|0\rangle - \beta|1\rangle)_B\\ &\quad + |\psi^+\rangle_{\tilde{A}A}(\alpha|1\rangle + \beta|0\rangle)_B + |\psi^-\rangle_{\tilde{A}A}(\alpha|1\rangle - \beta|0\rangle)_B].\end{aligned} \tag{3}$$

One can already see that the coefficients α and β, and hence Alice initial state $|\psi\rangle$ appears at Bob's side. We visualize this change of basis with help of a tetrahedron labeled in two equivalent ways, see figure 6. This does not mean, though, that Bob already possesses the state $|\psi\rangle$. In fact Bob's state is completely mixed, $\rho_B = \frac{1}{2}\mathbb{1}$ and contains no information. Any measurement yields a random outcome, which can be seen using the initial way of writing the state where Bob holds part of a maximally entangled pair. However, Alice can perform a (Bell) measurement on her part of the system, thereby projecting the superposition state equation (3) randomly into one out of the four possibilities. It follows that Bob must apply one of four possible correction operations, $\{\mathrm{id}, \sigma_x, \sigma_y, \sigma_z\}$, on his qubit to obtain the desired state. However, for this he needs to know the result of the Bell measurement, which has to be communicated classically. For instance, if Alice obtains the result $''|\psi^+\rangle''$, the resulting state after the measurement is given by $|\psi^+\rangle_{\tilde{A}A}(\alpha|1\rangle + \beta|0\rangle)_B$, and a σ_x correction operation that exchanges $|0\rangle \leftrightarrow |1\rangle$ is required at Bob's side to obtain $|\psi\rangle$ (and similarly for the other three possibilities). The teleportation process is visualized in figure 7. Notice that the state reduction takes place instantly—the measurement can be viewed as a change of our knowledge about the situation, where one of the four possibilities is randomly realized. However, without the classical information on the required correction operation, no quantum information was transmitted. This can also be illustrated with help of a virtual episode, the travel of Alice and Bob (see example 2.2.6, p 76 of [18]). One might look at a similar situation where a cake in a parcel is received—without the knowledge on how to orientate the parcel, opening it will result into crumbles. It is clear that this classical situation does not contain all relevant elements of the situation in question—in particular the proper orientation cannot be simply guessed, which would in the classical case result into a perfect, undisturbed cake.

We further remark that the location of Bob might be unknown. He simply needs to receive the classical information on measurement outcomes (which do not reveal any information about the teleported quantum state and must therefore not be transmitted secretly). In addition, the information carriers for input and output do not need to coincide. Furthermore, the qubit at Bob's side takes over completely the role of the teleported qubit. Importantly, all information about the teleported state at Alice side disappears, which is also necessary as to not violate the no-cloning theorem. If this qubit was initially entangled with a third system C, then finally Bob's qubit is entangled with C. This process is also refereed to as entanglement swapping (see figure 8), and plays an important role in the generation of long-distance entangled pairs for quantum communication. By teleporting individual qubits of a compound system, one can achieve the teleportation of a complex object. The problem of quantum communication is thus reduced to the problem of creating maximally entangled pairs of qubits in a quantum network.

4. Recent experiments and state-of-the-art

Quantum teleportation has fascinated physicists since it was introduced in 1993 [3]. It is thus not surprising that soon after the theoretic discovery, a first experimental demonstration was reported. Almost at the same time groups in Innsbruck and Rome demonstrate teleportation using photons [19, 20]. Quantum information was stored using the polarization degree of freedom of single photons. They used polarization entangled photons produced by a parametric down conversion source, together with polarizing beam splitters to implement an incomplete Bell measurement, where however teleportation succeeded only in 25% of all cases. Teleportation over large distances of up to 140 km was performed using photons [21–23], where one of the most prominent experiments demonstrated teleportation between two of the Canary islands [23]. Recently a similar experiment successfully showed long-distance entanglement swapping [24].

Similar experiments were later performed using light fields [25] and trapped ions [26, 27]. While the latter experiment demonstrated the full teleportation protocol deterministically, the teleportation was over short distance, between neighboring ions only. Teleportation between distant atomic systems [28], or using other information carriers such as quantum dots and solid-state qubits, but also teleportation between two different information carriers, such as between light fields and atomic ensembles [29], or from photons to solid-state qubits, where subsequently realized. For quantum communication over long distances, such quantum interfaces that allow one to map quantum information from one system to

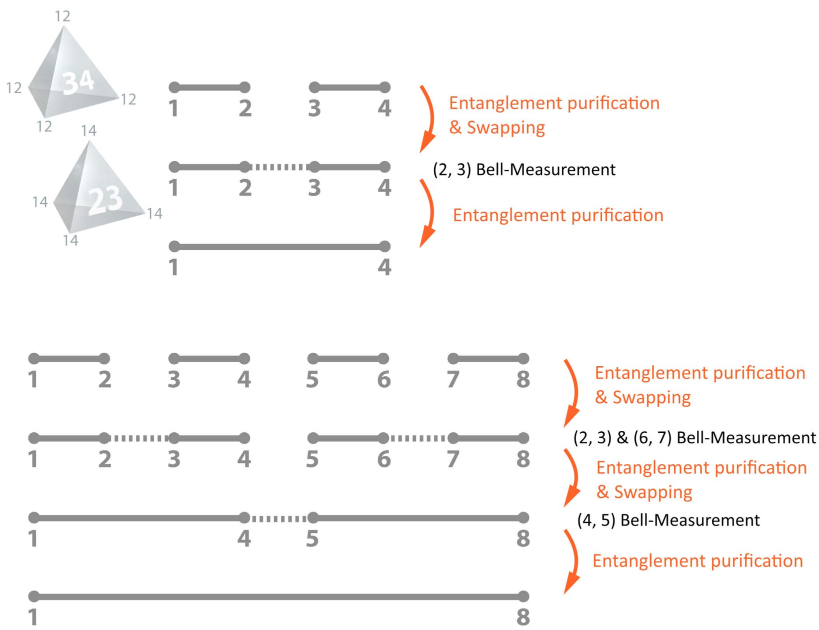

Figure 9. (Upper part) A high-fidelity entangled qubit pair (14) is generated using a combination of entanglement swapping and entanglement puririfcation of the short-distance elementary entangled pairs (12) and (34). (Lower part) Using a nested application of entanglement swapping and entanglement purification, one can generate long-distance entangled pairs. At each nesting level, the distance is at least doubled.

another play an important role. It is thus fair to say that teleportation is not an abstract possibility, but is already reality.

5. Long-distance quantum communication

As discussed earlier, the direct transmission of encoded quantum information has a rather large overhead in terms of resources, and suffers from very stringent error thresholds. Here we discuss an alternative where known, entangled quantum states are distributed that can be used as a resource for quantum communication via teleportation.

5.1. Quantum repeaters

The quantum repeater is a ground-based approach to long-distance quantum communication that will ideally use existing infrastructure, i.e. glass fiber networks. When sending single photon through a fiber (or free space), absorption and dephasing increase exponentially with the distance. This implies that for any practical purpose direct transmission is limited to a few hundred kilometers using existing fibers or transmission through air. To circumvent this problem, one can split the overall channel into short-distance segments and establish entangled pairs among these segments. Using entanglement swapping at each intermediate repeater station allows to generate a long-distance entangled pair. However, if the elementary pairs have non-unit fidelity or operations for entanglement swapping are noisy, the fidelity drops and only a few pairs can be connected this way. Still, this approach, also known as a quantum relay, already allows one to significantly increase the reachable distance.

For a scalable solution that allows for intercontinental distance communication, an additional process is required. One can generate from many identical copies of noisy entangled pairs (which can e.g. be generated by repeating the distribution of elementary entangled pairs) a smaller number of copies with increased fidelity probabilistically [30]. This process is called entanglement purification and in a sense allows to circumvent the no-cloning (or no-amplification) theorem since the desired states are known. A nested application of entanglement swapping and entanglement purification allows for the generation of entangled pairs over larger and larger distances [31, 32]. The overhead, i.e. the required number of elementary pairs or repetitions of the elementary creation process, scales only polynomially with the distance. This is illustrated in figure 9.

Nowadays huge theoretical and experimental efforts are devoted towards realizing a quantum repeater. While photons are the natural choice to transmit quantum information, they are hard to store and manipulate. Hence a central element for a repeater is an interface between flying qubits and storage qubits, e.g. ions or atomic ensembles. To take care of the probabilistic generation of elementary pairs (due to loss), and to realize entanglement swapping and purification, a quantum memory is required. While many of the building blocks for a quantum repeater have already been experimentally demonstrated [33, 34], the achieved fidelity are not yet sufficient to obtain a fully scalable scheme. Even the US Army is supporting experimental efforts in this direction, both in the US and Europe, since quantum cryptography can be realized using such a quantum communication network.

5.2. Satellite-based quantum communication

Ground-based quantum repeaters are however not the only method that is actively pursued. Satellite-based long-distance quantum communication [35] is not only discussed, but first experiments have already been performed. Using a (low-orbit) satellite, one only needs to to send a signal to the satellite through the atmosphere, where absorption and atmospheric fluctuations—together with focusing—are the main difficulties. The signal is then either processed, or transmitted to another ground station or the next satellite. Satellite-to-satellite communication is much more efficient, as there are no atmospheric disturbances or absorption.

Single photon transmission to and from a satellite, or to a moving aircraft, has been experimentally demonstrated [36–40]. The present scheme however requires to trust the satellite—and hence the provider, which is from a cryptographic perspective an unsatisfying situation. This limitation will however be overcome in future experiments, making such a satellite-based quantum communication a viable alternative.

6. Quantum networks: principles and experimental realizations

So far, we have been mainly concerned with direct communication between a single sender and receiver. However, a much more important and practical relevant task is the realization of a multi-user quantum communication network [8, 41]. The underlying principle could be a pairwise communication as discussed above, but also the direct distribution of multipartite entangled states [42]. Entanglement swapping can be used to obtain entangled states between pairs (or subgroups) of communication partners. When considering planar communication networks with probabilistic quantum channels, a perculation phenomenon—similar as in statistical physics—was discussed [43, 44].

However, it is fair to say that the investigation of the power and potential of quantum networks is at an early stage. In particular, using inherent quantum features such as multipartite entanglement or interference effects may open new and unexpected possibilities.

6.1. Quantum memories

A central element of a quantum networks are quantum memories which allow one to store quantum information. This is required not only for end-users, but also for intermediate repeater stations to e.g. realize entanglement-based long-distance communication. Storage of photons is a difficult task, and can only be achieved for short times using e.g. loops of fibers. Absorption and dephasing limit the length of delay loops, and given the large speed of light the achievable storage times. The speed of light can however be strongly reduced in certain materials, thereby effectively slowing or even halting a light pulse. This is known as electromagnetically induced transparancy or slow light [45, 46]. Other approaches include quantum memories based on atomic ensembles, where photonic states are transferred to atomic excitations, and vice versa. Such memories have been experimentally demonstrated, e.g. using rubidium atoms, and would be sufficient to realize a quantum relay. However, if one also needs to manipulate the stored quantum information, e.g. to perform entanglement purification, interfaces between photons and e.g. trapped ions, NV centers, superconducting interference devices or solid state qubits are more promising [34]. For instance, the high-fidelity manipulation of electronic states of trapped ions is highly advanced [6], where a fidelity of more than 99.9% can be achieved.

6.2. Quantum interfaces

Various systems for storing quantum information exist, and interfaces between light and atomic (or other) storage systems are being constructed [33, 34]. A promising candidate for a quantum interface is a single (or several) trapped ion(s) in a cavity. The photonic state is first transferred to the cavity mode, and then to the electronic state of the ion via appropriate laser pulses. Also a transfer in backward direction, including the coupling to a fiber, is possible and has already been experimentally demonstrated [34]. Currently, the success rates and the achievable fidelity are too low to allow for an application in a large-scale quantum network. This is however only a technological and not a principal challenge, and one can expect high-fidelity interfaces to be realized even with existing setups.

6.3. Operating quantum networks

Quantum cryptographic networks are not only discussed theoretically, but have been practically realized and tested [47–50]. In these experiments, which where e.g. performed in the USA, Japan, Austria and Switzerland, quantum key distribution was realized over large distances, over long periods of time and using existing infrastructure. For instance, the group of H Zbinden used the glass-fiber network of the Swiss telecom to realize key distribution between three partners, including the CERN, over 21 months [49]. In China, key distribution between three remote cities, over a distance of about 150 km, was demonstrated for a period of more than half a year [50]. While this is still far from a full-scale global communication network, it shows that quantum technologies are already at the edge of being utilized in practice.

7. Quantum internet—a context-based approach to quantum theory?

Quantum mechanics is one of the central physical theories and has perhaps more than any other theory changed our perception and description of nature. This is mainly due to its counter-intuitive features that contradict our everyday experiences. While quantum mechanics is taught at undergraduate and high school level, its abstract nature and advanced mathematics make it a difficult topics where in contrast to topics from classical physics no established and generally accepted curriculum and ways to teach it are established yet. This might also be due to lack of obvious direct connection to contexts of daily life, from which other topics such as classical mechanics or electrodynamics highly benefit.

We suggest to substitute this context by the treatment of a modern research topic that has a high has sociological importance: actual and future technology to ensure secure communication in the world wide web. Understanding the basic building blocks of the quantum internet can be the anchor and unifying theme to learn quantum mechanics [51]. Following a quantum information approach to quantum mechanics [9–13], one can first treat single- and two-qubit stystems to illustrate central features of quantum mechanics, and emphasize the differences to classical physics. The basic idea of this approach is to use the simplest quantum system—the qubit—to illustrate the basic features of quantum mechanics, rather than more complex or complicated objects such as atoms that are described by (infinite-dimensional) wavefunctions and partial differential equations. In all cases, we believe it is of vital importance use visualizations to promote the understanding of the core ideas before (complex) mathematics is introduced. In a quantum information approach, such visualizations exist: for example the Bloch sphere representation and visualization for the measurement, but also for other processes and schemes [9–13]. Quantum cryptography and teleportation can then serve as relevant examples for technological applications of the basic concepts, and other selected topics that are of relevance for a quantum internet can be treated. In particular, the highly relevant topic of secret data transmission can be discussed in the context of society.

8. Summary and outlook

A quantum internet with all its possible applications might sound like science fiction on a first thought, however a realization is technologically possible and far less challenging than e.g. a full-scale quantum computer. Crucial building blocks and even small-scale networks have already been demonstrated, and e.g. quantum cryptography devices are already commercially available. Possible applications of such a quantum network for the transmission of quantum states include networks of detectors and clocks with application in fundamental research and distributed quantum computation. The main motivation to realize such a network at present is quantum cryptography, which ensures provable secure communication which is not only desirable for banks and governments, but also for the home user. Internet shopping and mobile banking are just two applications where security is paramount. The coming years will show whether the future development of the quantum internet is governed by secret agencies and governments, by commercial companies, or by civil research institutions. Free access to secure and secret communication—without back-doors for intelligence service—is thought as a basic right and part of the individual freedom by many citizens. Whether this can be ensured —or even is a worthwhile goal in times where also lack of information can be harmful—will be among the central questions in the upcoming years. What is clear, though, is that the classical internet would look quite different today if the development had not been the (unexpected) result of fundamental research, but would have been lead by the military or by governments.

Acknowledgments

This work was supported by the Austrian Science Fund (FWF): P28000-N27. An article dealing with a similar topic (in German) was published by two of the present authors in [52]. We are grateful to Dipl-Des. Michael Tewiele for the realization of the images in this paper.

References

[1] Gisin N and Thew R 2007 Quantum communication *Nat. Photon.* **1** 165–71
[2] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (New York: Cambridge University Press) 2010: 10th anniversary edn
[3] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels *Phys. Rev. Lett.* **70** 1895–9
[4] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography *Rev. Mod. Phys.* **74** 145–95
[5] Schrödinger E 1935 The present status of quantum mechanics *Naturwissenschaften* **23** 1–26
[6] Wineland D J 2013 Nobel lecture: superposition, entanglement, and raising Schrödinger's cat *Rev. Mod. Phys.* **85** 1103–14
[7] Haroche S 2013 Nobel lecture: controlling photons in a box and exploring the quantum to classical boundary *Rev. Mod. Phys.* **85** 1083–102
[8] Kimble H J 2008 The quantum internet *Nature* **453** 1023–30
[9] Dür W and Heusler S 2013 What we can learn about quantum physics from a single qubit arXiv:1312.1463
[10] Dür W and Heusler S 2014 Visualization of the invisible: the qubit as key to quantum physics *Phys. Teach.* **52** 489–92
[11] Dür W and Heusler S 2016 The qubit as key to quantum physics part II: Physical realizations and applications *Phys. Teach.* **54** 156–9
[12] Dür W and Heusler S 2012 Was man vom einzelnen Qubit über Quantenphysik lernen kann *PhyDid* A **11** 1–16
[13] Dür W and Heusler S 2014 Was man von zwei Qubits über Quantenphysik lernen kann: Verschränkung und Quantenkorrelationen *PhyDid* A **13** 11–34
[14] Hensen B *et al* 2015 Loophole-free Bell inequality violation using electron spins separated by 1.3 km *Nature* **526** 682–6
[15] Komar P, Kessler E M, Bishof M, Jiang L, Sorensen A S, Ye J and Lukin M D 2014 A quantum network of clocks *Nat. Phys.* **10** 582–7
[16] Zwerger M, Briegel H J and Dür W 2016 Measurement-based quantum communication *Appl. Phys.* B **122** 1–15
[17] Putzer K 2014 Quantenteleporation für den Schulunterricht *Diploma Thesis* University of Innsbruck, Austria (in German; see also https://prezi.com/oalboaiidsbd/)
[18] Gruska J 1999 *Quantum Computing* (Berkshire: McGraw-Hill International)
[19] Bouwmeester D, Pan J-W, Mattle K, Eibl M, Weinfurter H and Zeilinger A 1997 Experimental quantum teleportation *Nature* **390** 575–9
[20] Boschi D, Branca S, De Martini F, Hardy L and Popescu S 1998 Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels *Phys. Rev. Lett.* **80** 1121–5
[21] Marcikic I, de Riedmatten H, Tittel W, Zbinden H and Gisin N 2003 Long-distance teleportation of qubits at telecommunication wavelengths *Nature* **421** 509–13
[22] Jin X-M *et al* 2010 Experimental free-space quantum teleportation *Nat. Photon.* **4** 376–81
[23] Ma X-S *et al* 2012 Quantum teleportation over 143 km using active feed-forward *Nature* **489** 269–73

[24] Herbst T, Scheidl T, Fink M, Handsteiner J, Wittmann B, Ursin R and Zeilinger A 2015 Teleportation of entanglement over 143 km *Proc. Natl Acad. Sci.* **112** 14202–5
[25] Furusawa A, Sørensen J L, Braunstein S L, Fuchs C A, Kimble H J and Polzik E S 1998 Unconditional quantum teleportation *Science* **282** 706–9
[26] Riebe M *et al* 2004 Deterministic quantum teleportation with atoms *Nature* **429** 734–7
[27] Barrett M D *et al* 2004 Deterministic quantum teleportation of atomic qubits *Nature* **429** 737–9
[28] Krauter H, Salart D, Muschik C A, Petersen J M, Shen H, Fernholz T and Polzik E S 2013 Deterministic quantum teleportation between distant atomic objects *Nat. Phys.* **9** 400–4
[29] Sherson J F, Krauter H, Olsson R K, Julsgaard B, Hammerer K, Cirac I and Polzik E S 2006 Quantum teleportation between light and matter *Nature* **443** 557–60
[30] Dür W and Briegel H J 2007 Entanglement purification and quantum error correction *Rep. Prog. Phys.* **70** 1381
[31] Briegel H-J, Dür W, Cirac J I and Zoller P 1998 Quantum repeaters: the role of imperfect local operations in quantum communication *Phys. Rev. Lett.* **81** 5932–5
[32] Sangouard N, Simon C, de Riedmatten H and Gisin N 2011 Quantum repeaters based on atomic ensembles and linear optics *Rev. Mod. Phys.* **83** 33–80
[33] Hammerer K, Sørensen A S and Polzik E S 2010 Quantum interface between light and atomic ensembles *Rev. Mod. Phys.* **82** 1041–93
[34] Northup T E and Blatt R 2014 Quantum information transfer using photons *Nat. Photon.* **8** 356–63
[35] Jennewein T and Higgins B 2013 Quantum space race *Phys. World* **26** 5256
[36] Wang J-Y *et al* 2013 Direct and full-scale experimental verifications towards ground-satellite quantum key distribution *Nat. Photon.* **7** 387–93
[37] Nauerth S, Moll F, Rau M, Fuchs C, Horwath J, Frick S and Weinfurter H 2013 Air-to-ground quantum communication *Nat. Photon.* **7** 382–6
[38] Yin J *et al* 2013 Experimental quasi-single-photon transmission from satellite to earth *Opt. Express* **21** 20032–40
[39] Vallone G, Bacco D, Dequal D, Gaiarin S, Luceri V, Bianco G and Villoresi P 2015 Experimental satellite quantum communications *Phys. Rev. Lett.* **115** 040502
[40] Pugh C J *et al* 2016 Airborne demonstration of a quantum key distribution receiver payload arXiv:1612.06396
[41] Duan L-M and Monroe C 2010 Colloquium: quantum networks with trapped ions *Rev. Mod. Phys.* **82** 1209–24
[42] Wallnöfer J, Zwerger M, Muschik C, Sangouard N and Dür W 2016 Two-dimensional quantum repeaters *Phys. Rev.* A **94** 052307
[43] Perseguers S, Lewenstein M, Acin A and Cirac J I 2010 Quantum random networks *Nat. Phys.* **6** 539–43
[44] Perseguers S, Lapeyre G J Jr, Cavalcanti D, Lewenstein M and Acin A 2013 Distribution of entanglement in large-scale quantum networks *Rep. Prog. Phys.* **76** 096001
[45] Harris S E 1997 Electromagnetically induced transparency *Phys. Today* **50** 36–42
[46] Fleischhauer M, Imamoglu A and Marangos J P 2005 Electromagnetically induced transparency: optics in coherent media *Rev. Mod. Phys.* **77** 633–73
[47] Peev M *et al* 2009 The SECOQC quantum key distribution network in Vienna *New J. Phys.* **11** 075001
[48] Sasaki M *et al* 2011 Field test of quantum key distribution in the Tokyo QKD network *Opt. Express* **19** 10387–409
[49] Stucki D *et al* 2011 Long-term performance of the SwissQuantum quantum key distribution network in a field environment *New J. Phys.* **13** 123001
[50] Wang S *et al* 2014 Field and long-term demonstration of a wide area quantum key distribution network *Opt. Express* **22** 21739–56
[51] Lamprecht R 2015 Quantennetzwerke—Ein kompetenzorientierter Zugang zur Quantenphysik für den Unterricht *Diploma Thesis* University of Innsbruck Austria (in German)
[52] Dür W and Heusler S 2016 Das Quanteninternet *Prax. Naturwissenschaften: Phys. Schule* **65** 23–32